Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1324 06/17/11

~ Hacks Are Entertainment! ~ People Are Talking! ~ Anonymous Is Detained!

~ Japan After Virus Makers ~ Jobs Gets Comic Book! ~ New MacBook Air Soon!

~ JK Rowling’s Pottermore! ~ Cork the Bubble Talk! ~ PDF Integration!
~ Juror Gets Jail for Chat ~ Social Networking Ages ~ Web Name Shake-up?

-* "Hacktivists" Make Some Noise *-
-* Training, Monitoring Is Necessary! *-
-* World Leaders: Put Cyber Security on Agenda *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

GO Bruins!! Congratulations to another Boston sports team taking home a championship - that’s all four major teams in Boston winning it all within the past ten years! Don’t get me wrong (or is it right?), I’m not a huge sports fan these days. I used to be, when money didn’t play a major factor in sports, but my enthusiasm waned over the years. But that doesn’t mean that I don’t support my local teams. It’s hard not to while remembering great Boston teams from yesteryear - many of whom I managed to see when I was younger. So, I feel that a Stanley Cup win for the Boston Bruins is grounds for excitement - especially after a 39-year hiatus!

I had my spinal injection earlier in the week - a walk in the park, after hearing all of the "painful" hype up to that point. Once I got in to a room, it took all of maybe 5 minutes. I was told that I would likely not feel any relief for a minimum of 48 hours, and up to two weeks, if anything at all. I was also told that it would probably take one or two more treatments to see some relief, so I’ll see how things go. So for a few days, I had a mini-vacation of sorts to give the treatment an opportunity to take hold.

So, I’ll continue to take it relatively easy for another day or so, and hope that I get some relief. Meanwhile, let’s move on to another week of A-ONE - enjoy!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Battlefield 3 Takes Aim at Modern Warfare 3!
""""""""""""""""""""""""""""""" Gamers Gripping Handheld Controls!
Sega Pass System Hacked, Offline!

=~=~=~=

'Battlefield 3' Takes Aim at 'Modern Warfare 3'

Beyond the flashing flatscreens, blaring speakers and "booth babes" at last week's Electronic Entertainment Expo, there was no bigger showdown at the video game industry's annual extravaganza than the one brewing between "Call of Duty: Modern Warfare 3" from Activision Blizzard Inc. and "Battlefield 3" from Electronic Arts Inc.

For the past four years, Activision reigned supreme with its "Call of Duty" franchise, breaking game sales records and earning critical acclaim for its polished shoot-'em-up realism. The Santa Monica, Calif.-based publisher may finally have a worthy adversary when EA releases "Battlefield 3" on Oct. 25, two weeks before "Modern Warfare 3" comes out Nov. 8.

"Naturally, it's good for the consumers to have one of these heavyweight fights that's going on right now," said Karl-Magnus Troedsson, general manager at Stockholm, Sweden-based "Battlefield 3" developer DICE. "The objective isn't winning for the competition; it's about winning over ourselves, to ensure that we make the best game that we have ever done."

While the goal of "Call of Duty" and "Battlefield" is the same - shoot combatants, preferably in the head - when their newest sequels are released this fall, they will share several other similarities. Most notably, both are set amid modern-day worldwide conflicts with soldiers fighting on expansive urban battlegrounds in such cities as Paris and New York.

DICE developers are plotting for "Battlefield 3" to look sleeker than previous editions. They've developed a new version of their Frostbite game engine to craft the sequel, which promises more realistic graphics, fuller sound and amplified environmental destruction. The engine is also being used to create the racing game "Need for Speed: The Run."

"With our new Frostbite 2 technology, we feel like we have a strong offering," said Frank Gibeau, president of EA Games. "We're a generation ahead of what's out there. It looks spectacular. From a marketing standpoint, we're going all out. We're going to spend a lot of money. It'll probably be the biggest budget for the company this year - if not ever."

During E3, at the front of the Los Angeles Convention Center's South Hall, EA previewed a "Battlefield 3" multiplayer level set within the tunnels and streets of Paris. Meanwhile, at the back of the sprawling expo, Activision showed off a "Modern Warfare 3" co-op level that tasked players with surviving waves of enemies, including suicide bomber dogs.

"If 'Call of Duty: Modern Warfare 3' is a Hollywood-ish action play, 'Battlefield 3' is more like a documentary," tweeted Hideo Kojima, the Tokyo, Japan-based developer behind the third-person "Metal Gear" franchise. "While play-related rail games are the mainstream after the success of 'Call of Duty' and 'Uncharted,' this stoic attitude is fresh."

Throughout most of the last decade, EA and Activision were equal rivals when it came to military shooters, regularly deploying new chapters in their respective World War II franchises, beginning with the original "Medal of Honor" in 1999 and "Call of Duty" in 2003, but Activision was the first to recognize gamers had grown bored of blasting Nazis.

With the release of developer Infinity Ward's "Call of Duty 4: Modern Warfare" in 2007, Activision brought the battle to the 21st century. The contemporary iteration introduced terrorists as adversaries and laser-sighted rifles as weapons. The leap forward paid off. It was the best-selling game of that year, going on to sell more than 13 million copies.

Activision continued to dominate in 2009 with "Modern Warfare 2," which sold more than 20 million copies. The hype also helped propel editions by Treyarch, the other studio developing "Call of Duty" games, to the top of sales charts. Treyarch's Cold War-era "Call of Duty: Black Ops" has sold more than 22 million copies worldwide since last year's launch.

The "Battlefield" franchise, which has always been geared more toward PC than console gamers, lacks the same firepower as "Call of Duty." The last full-fledged "Battlefield" game, last year's "Battlefield: Bad Company 2," sold a respectable number of copies: more than seven million, which seems small when compared to the staggering haul taken by "Call of Duty."

"'Battlefield' wants to take them on directly, but they're trying to do it through innovation, and I don't know if that's necessary," said Brian Crecente, editor of gaming blog Kotaku. "I think it's more about polish and delivering an experience that can really be replayed online. That's where 'Battlefield' is going to have to take on 'Modern Warfare 3.'"

"Modern Warfare 3" is again being developed by Encino, Calif.-based Infinity Ward, but this time in tandem with San Francisco-based Sledgehammer Games and Madison, Wis.-based Raven Software, which is working on the game's online multiplayer mode. The collaborative approach to developing the third "Modern Warfare" installment could prove hazardous.

Adam Sessler, host and editorial director of G4's gaming series "X-Play," said sales of "Modern Warfare 3" definitely won't tank but bad buzz that the "Call of Duty" saga is becoming repetitive might affect the franchise, especially after Activision ousted the heads of Infinity Ward and several other employees followed them out the door last year.

"The three words 'Call of Duty' almost ensure a certain number of sales," said Sessler. "I could see this being the beginning of a decline. I don't know what the quality of the game will be. It should be just fine, but this is from a new Infinity Ward, so whether they hold to the standard established with the first two 'Modern Warfare' games is uncertain."

EA already unsuccessfully attempted to shoot down the "Call of Duty" juggernaut last year by perking up its "Medal of Honor" series with a present-day Afghanistan chapter that only sold about four million copies. The praise that "Battlefield 3" earned from this year's E3 attendees might mean that EA could actually make a dent in the armor of "Call of Duty" this time.

"We know the competition is out there," said Glen Schofield, general manager at Sledgehammer Games. "It’s really about how we’re going to make these millions and millions of fans - who write in and talk to us every day through emails, tweets, everything - how are we going to make the millions of fans happy, not how are we going to beat the other guys."

Gamers Gripping Handheld Controls

Even though motion-sensing videogame controllers are all the rage, sometimes a player prefers a Batarang for bashing bad guys.

Accessory titan Power A is seeing keen interest in a console controller it designed similar to a throwing weapon in the arsenal of DC Comics crime fighter Batman even though it doesn’t hit the market until later this year.

Batarang controllers timed to hit with the release later this year of a sequel to Warner Brothers blockbuster Batman videogame will join a strong-selling array if accessories are created by the US-based firm.

"I don’t see videogames ever going to a point where people aren’t going to want to pick up a controller and shoot and punch and do things of that nature," Power A divisional vice president of product development John Moore told AFP.

"I don’t think they are going away... They are here to stay."

Nintendo is credited with opening the world of videogames to moms, seniors and other "casual gamers" with the launch of the Wii console in 2006.

Microsoft built on the trend last year by adding gesture and voice controls to Xbox 360 consoles with Kinect, and Sony released a motion-sensing Move accessory for PlayStation 3 (PS3).

Motion controls are a hit, with millions of Kinect and Move devices being snapped up by a broadening audience of gamers.

Many of those "casual" players will be lured to titles calling for toggles, buttons and other features on traditional controllers, according to Moore.

"Kinect is awesome because it brought people into gaming who wouldn’t necessarily consider gaming before," Moore said.

"But I think people are always going to want to have controller that they can kick back and play... Not everyone wants to get up and jump around and dance."

And as consoles get more sophisticated, and multi-player games more popular, the number of people playing simultaneously should climb - driving up the demand for controllers.

With tens of millions of consoles in homes around the world, the market for replacement, spare or vanity controllers is enticing for makers of videogame accessories.

"The controller market is absolutely huge," Moore said.

Power A makes miniature controllers; versions of the gadgets based on Lego videogames, and even models with built in fans to cool hands grown hot from hours of playing intense shooter titles such as "Call of Duty."

The Batarang controller sprang from a relationship with Warner Brothers, and Moore’s love of the first Batman videogame, which he admitted to playing through several times.

Washington state-based Power A was among myriad accessory makers showing off new creations and forming alliances at a recent Electronic Entertainment Expo in Los Angeles.

Plantronics and Turtle Beach were in the ranks of companies that showcased headsets that immerse players in rich sound while allowing them to chat with opponents or allies in online games.

Turtle Beach billed its new Ear Force PX5 model priced at $250 as the most advanced headset for Xbox 360 or PS3 consoles.

Accessories ranged from giant screens and wireless steering wheel controllers to cables for quickly routing massive amounts of game data and wall-mounted racks for organizing gear.

Sega’s Sega Pass System Hacked, Offline

Sega’s Sega Pass database was hacked and has remained offline since Thursday, reports said, adding to the list of game developers and other companies whose security has been compromised.

The system has been down since Thursday, according to an email reportedly sent to the members of the system. That email was reprinted by PlayStationLifeStyle.net.

Messages left with members of Sega’s public-relations team were not returned by press time.

"As you may be aware, the SEGA Pass system has been offline since yesterday, Thursday 16 June," the email begins. "Over the last 24 hours we have identified that unauthorised entry was gained to our SEGA Pass database.

"We have identified that a subset of SEGA Pass members emails addresses, dates of birth and encrypted passwords were obtained," Sega added. "To stress, none of the passwords obtained were stored in plain text."

Payment information was not compromised, according to the memo that PlayStationLifeStyle.net published, as Sega uses external payment providers. Sega automatically reset user passwords, it said, but warned users to be suspicious of emails that ask for personal information.

Sega Pass serves as a way for Sega to distribute free content to customers, including demos and mini-games, plus a monthly newsletter and a support line. It is free to join, although the Sega Pass site was down at press time.

In its place, Sega posted a message: "SEGA Pass is going through some improvements so is currently unavailable for new members to join or existing members to modify their details including resetting passwords," Sega said. "We hope to be back up and running very soon. Thank you for your paitence [sic]."

The Sega forums were also offline to "carry out some essential maintenance," a note posted on the site said.

It wasn't immediately clear who, if anyone, took credit for the hack.

LulzSec, which has targeted gaming company Bethesda Softworks, the Web site for CCP Games' EVE Online as well as Minecraft and Escapist Magazine, has attacked gaming companies at the behest of a call-in line.

But the LulzSec Twitter account was silent Friday, after an all-day session in which the group's representative or members sent messages to supporters after LulzSec leaked about 62,000 usernames and passwords

However, LulzSec denied responsibility. "@Sega - contact us. We want to help you destroy the hackers that attacked you. We love the Dreamcast, these people are going down," the group posted on its Twitter feed.

Meanwhile, Spanish police have arrested alleged "Anonymous" members, followed by 32 more arrests by Turkish police.

On Friday, the only message on the AnonOps Web site was a message condemning censorship by the Turkish government.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

World Leaders Should Put Cyber Security on Agenda

World leaders should put cyber security on the international agenda at forums such as the G20 and bring pressure to bear on "slower-moving" nations to take a stand against hacking, the co-founder of a global industry body said on Tuesday.

Peter Coroneos, co-founder of the International Internet Industry Association and head of Australia's industry body, said such leadership by major powers could support and hasten early industry efforts to adopt global anti-hacking safeguards.

"Getting the issue elevated to a level like the G20 would be a good way to promote engagement with economies that might otherwise move a little slower," Coroneos told Reuters.

"We saw that with the nuclear arms limitation treaty, where you did have a couple of early movers," he added.

Recent cyber attacks on multinational firms and institutions, from Google and Citigroup to the International Monetary Fund, have raised fears that governments and the private sector are losing the battle against hackers.

Google pointed the finger at China for an attempt to gain access to the Gmail accounts of assorted activists, and global miner BHP Billiton has also harbored concerns about high-tech espionage from China and its rivals.

Coroneos did not want to discuss any Chinese role in such hacking, but said hackers typically used networks of "zombie" personal computers, unprotected machines in homes anywhere in the world, to launch their attacks on secure databases.

"It’s really the weapon of choice," he said.

Australia has taken a lead in forming a government and private-sector partnership to combat cyber hacking, announcing plans to draw up a cyber defense strategy and backing a campaign by Internet service providers to eradicate zombie computers.

Australian ISPs recently adopted a code of practice designed to identify and fix zombie computers with techniques such as monitoring for unusual activity in normally dormant periods, such as overnight when users are usually asleep.

The users are notified of any suspicious activity, without breaching privacy, and are also told how to secure their computers, either by themselves or with professional help.

"In the first six months of its operation, 90 percent of the ISP user base is security compliant," Coroneos said.

Australia’s Internet Industry Association, which represents local ISPs, is now working with Internet associations in other countries to develop similar codes overseas, Coroneos said.

"If we want to really tackle it effectively we have to tackle it in multiple jurisdictions simultaneously around the world," he said, adding that ISP groups in the United States, Europe, India and Argentina were now looking at the Australian code as a basis for international cooperation.

"We have started to have a dialogue to see if this is something we can do in a coordinated way," Coroneos said.

"Hacktivists" Make Noise on Government Websites

A breed of cyber pranksters known as "hacktivists" appears to be on a campaign to embarrass the U.S. government, but such types of attack are unlikely to breach the computer firewalls that protect important official secrets, independent analysts say.

A loosely organized group of hackers called Lulz Security, little known outside of cybersecurity circles, has claimed attacks against the public websites of the CIA and U.S. Senate over the past week. Hackers mounted

a second, similar assault against the Senate website on Wednesday, possibly the work of copycats.

U.S. officials say government computer systems and websites, including those operated by the Pentagon, are subjected to thousands of attempted hackings each month but that safeguards usually keep would-be intruders away from sensitive data.

The Lulz style of attack, known as a denial of service meant to disable the target's website, is often undertaken by activists as young as teenagers and pose little danger aside from embarrassment and website clean-up costs that can run into the hundreds of thousands of dollars.

"It's hacktivism - activism through hacking. Campaigns of this kind have been done in the past for two reasons: outrage and self-promotion. This one is some combination of those," said Alan Paller, director of research at the SANS Institute, a think tank devoted to cyber issues.

"There's a lot of noise but no real downside, except that if people don't think the CIA can protect its own website, it colors their thinking about what it can do in other arenas - maybe unfairly, but it doesn't really matter."

Denial of service attacks are the most basic form of cyber intervention, in which hackers jam a website by flooding it with traffic. The attacks often involve software that can be downloaded for free from the Internet.

A CIA spokeswoman said: "The CIA's public website experienced technical issues that caused it to respond slowly for a short time yesterday evening. Those issues are now resolved. These technical issues affected only the CIA's unclassified public website. Our classified systems were not affected."

But federal authorities take hacktivism seriously, as a kind of vandalism that represents the less dangerous edge of a cyber security spectrum that includes hacking by foreign military operatives, economic spies, organized criminals and terrorists.

"It effects everything from national security to commerce, all the way down to individuals. You've got a lot of identity theft. So we're not saying that's no big deal. We're looking at it across the board," said a U.S. official who spoke on condition of anonymity.

Far more serious are recent hackings at Google, Lockheed Martin Corp and the International Monetary Fund, in which analysts say professional hackers may have tried to steal secrets on behalf of powerful interests, including national governments.

Google raised the alarm about cyber attacks in Washington earlier this month when it disclosed that hackers, perhaps from China, had sought access to the Gmail accounts of senior U.S. officials.

U.S. Secretary of State Hillary Clinton weighed into the controversy by calling the allegations serious and under investigation by federal authorities.

Defense contractor Lockheed Martin also reported thwarting an attack on its information systems network that cyber security experts believe may have originated in China.

"The real burglars are stealthy, and often in those cases, you don’t know what they took," said James Lewis of the Center for Strategic and International Studies.

"Nobody who is serious would do a denial of service attack. It would be like burglars hiring a marching band," he said.

Turkish Police Detain Anonymous Members

Turkish police detained 32 members of the Anonymous cyberactivism collective on suspicion of planning attacks on a number of websites, Turkish state-run news agency Anatolian reported.

The action came in response to a complaint from Turkey’s Directorate of Telecommunications, whose website was taken down on Thursday as part of a protest against what Anonymous says is government censorship of the Internet.

Turkey, whose ruling AK Party won a parliamentary vote on Sunday, plans to introduce a new Internet filtering system in August, under which users will have to sign up for one of four filters - domestic, family, children and standard.

Anonymous, a loose activist collective which has attacked many websites including those of Amazon and Mastercard in the name of Internet freedom, says the system will make it possible to keep records of people’s online activity.

Eight of the 32 suspected cyberactivists detained on Sunday were minors, Anatolian said.

The police operation in Turkey follows the arrest of three so-called Anons in Spain on Friday on suspicion on organizing cyber attacks against the websites of Sony, banks and governments.

Anonymous said on its website (www.anonops.blogspot.com) and on a video posted on YouTube that the arrest had not shut down the leadership of its operations as claimed, because the group had no centralized leadership.

The group said it had taken down the Spanish national police website for some hours on Saturday in retaliation.

It said the arrests were part of a police attempt to distract attention from protesters dispersing in cities across Spain at the weekend after four weeks demonstrating against government austerity, reforms and unemployment.

The video featured a figure wearing the Guy Fawkes mask made popular by the graphic novel "V for Vendetta" which the group is known for wearing and expressed sympathy with the protesters, known as "indignados" (or indignant).

Anonymous members cripple websites by overwhelming their servers with traffic in so-called denial of service attacks. The group publicizes these campaigns on the Web, giving supporters the information to attack a targeted site.

Cyber Raids Fuel Calls for Training, Monitoring

Employers rushing to boost cyber defences after a rash of U.S. online break-ins won’t block spies and thieves by simply throwing technology at the problem, since their core weakness is often badly-trained and -managed workers.

In the cyber realm, as in other areas of security, the human factor is a pervasive vulnerability, be it theft by malicious "insiders" or inadvertent breaches by employees clicking on a compromised link, analysts say.

More rigorous training may not end the abuse of corporate cyber systems - the sophistication of some hacker tactics is so great that 100 percent security is probably unattainable - but it can significantly reduce the risks, specialists say.

The same goes for the adoption of intrusive new ways of monitoring employee online behavior and compliance with good cyber practice, some security specialists say.

"(High-tech) Bells and whistles are no use if you don’t have trusted, loyal and well-informed staff," said an industry executive who spoke recently at a closed door cyber seminar.

Many experts say much more can be done to tighten security at the "endpoint" - in other words, people - rather than place excessive reliance on clever software, important as that is.

Some experts see a need to carry out security vetting when hiring key staff, for example computer system administrators.

"Technology is only a part of the problem - all systems are composed of people, processes and technology - you only need to break one of the components to attack the system," said Steve Purser, a senior expert at the European Network and Information Security Agency, a European Union body.

He said there were no hard and fast rules about monitoring staff online because data differed in sensitivity and context.

"The important point is to communicate the rules to staff and to ensure that the rules are being followed," he said.

The need is urgent, not least because employers are worried recession may swell the ranks of staff in line for retrenchment who plan to take proprietary data with them out of the door.

Some are queasy about the notion of intruding on employees’ online work. But then, analysts note, hackers are doing exactly the same thing - and imperiling jobs into the bargain.

"It’s the people side of the equation that is letting the bad guys through right now," Neil Fisher, Vice President of Global Security Solutions at Unisys Corp told Reuters.

He was referring to ’phishing’ attacks, a hacker ploy to obtain data

such as passwords or bank details by posing as a legitimate institution.

In advanced "spear-phishing" campaigns hackers craft personalized e-mails, often using data available on social media websites, duping recipients into downloading attachments that launch malicious software that takes over their computers.

Such ploys are suspected in at least some recent prominent attacks, which have targeted entities such as the International Monetary Fund, Central Intelligence Agency, the U.S. Senate, and companies such as Citigroup and Lockheed Martin.

Mohan Koo, CEO of Dtex Systems (UK), said most organizations tended to over-prioritize the risk of external threats, a tendency he said was prevalent in the financial sector.

"For years now investment banks have lived by the motto Know Your Customer' today it's more critical that they focus on Know Your Insider' because that is where they have a weakness."

"The problem is that most organizations don't monitor their insiders with a sufficient level of granularity to quantify the threat to their business. If they did, the shock would be sufficient to spark a significant change in their approach."

A March 28 study by computer security firm McAfee and U.S. government consulting company SAIC said the most significant threat reported by organizations when protecting information was data leaked accidentally or intentionally by employees.

The risk of malicious theft of data or intellectual property by insiders for private gain or to boost value to potential new employers may rise as Western economies struggle, analysts say.

A 2011 survey of cyber crime by Verizon, the U.S. Secret Service and the Dutch High Tech Crime Unit noted concern among industry experts that financial strain would cause an increase in insider abuse, although evidence was sparse so far.

An 2010 Imperva cyber security company study of 1,026 people in several business districts in London showed that if rumors were circulating about possible redundancies, 37 percent of respondents said they would want to take information with them.

Tony Dyhouse, a security expert at Britain's ICT Knowledge Transfer Network, told Reuters a lot of the insider threat was actually "from people who are no longer inside."

"They've left the company but they still have access credentials, they may still have site passes and computer access. All too often people leave the company and their accounts are not closed down.

"People are aware of the value of data and they will try and keep things and send information home. They actually take preemptive action, so 'now I am going to get my own back, or at least I am going to make sure I have the capability to do so'." (Editing by Philippa Fletcher)

Japan To Fine Or Jail Computer Virus Creators

Japan will punish people who create or wilfully spread computer viruses with fines and prison terms of up to three years under a new law enacted by parliament.

Under the law, police can seize email communication logs of suspects from Internet service providers, among other information.

The action, which has met with opposition from privacy and free speech advocates, brings Japan a step closer to concluding the Convention on Cybercrime, a Europe-led effort.

The convention is the first international treaty to combat crimes committed via the Internet and other computer networks. Japan has signed the treaty but must pass relevant domestic laws to conclude it.

Under Japan’s new law, people who create or distribute a computer virus with no justifiable reason face prison terms up to three years or fines up to 500,000 yen (6,200 dollars).

Those who deliberately store a computer virus face up to two years in prison or fines up to 300,000 yen.

Japanese police agencies had long pushed for such a law, but past bills failed amid strong criticism from privacy and freedom-of-speech advocates who have warned of excessive police powers.

The text of the law says that "in view of the realities of cyber crime associated with the advancement of information processing ... it is necessary to develop the necessary regulations".

Because of concerns the law could violate the privacy of communications guaranteed under the Japanese constitution, it includes a resolution that urges authorities to apply the law appropriately.

Lulz Hackers Say Attacks Are Entertainment

Computer hackers who have hit the websites of the CIA, US Senate, Sony and others during a month-long rampage said Friday that they were staging the attacks for their own entertainment.

"You find it funny to watch havoc unfold, and we find it funny to cause it," the hacker group known as Lulz Security said in a 750-word online "manifesto."

"For the past month and a bit, we’ve been causing mayhem and chaos throughout the Internet, attacking several targets including PBS, Sony, Fox, porn websites, FBI, CIA, the US government, Sony some more, online gaming servers," Lulz said.

"While we’ve gained many, many supporters, we do have a mass of enemies, albeit mainly gamers," Lulz said, adding that they were not concerned.

"This is the lulz lizard era, where we do things just because we find it entertaining," said Lulz, whose name is a derivative of the text shorthand for LOL, or "laugh out loud."

"This is the Internet, where we screw each other over for a jolt of satisfaction," the group said.

"We release personal data so that equally evil people can entertain us with what they do with it," Lulz said. "And that's all there is to it, that's what appeals to our Internet generation.

"We're attracted to fast-changing scenarios, we can't stand repetitiveness, and we want our shot of entertainment or we just go and browse something else, like an unimpressed zombie," Lulz said.

The group said it will "continue creating things that are exciting and new until we're brought to justice, which we might well be."

Lulz has released tens of thousands of user names and passwords in recent weeks but the group said Friday they were "sitting on" the personal information of 200,000 users of the Brink videogame.

"It might make you feel safe knowing we told you, so that Brink users may change their passwords," Lulz said.

On Wednesday, Lulz knocked the CIA's public website, cia.gov, out of commission for about two hours.

Lulz, in a message on their Twitter feed @LulzSec on Friday, also denied reports that they were in conflict with the hacker group Anonymous, from which Lulz is believed to have formed.

"To confirm, we aren't going after Anonymous," Lulz said.

Anonymous has been staging cyberattacks for years on companies cracking down on music and movie piracy and gained notoriety last year with cyberattacks in support of controversial website WikiLeaks.

New MacBook Air 'To Hit Market This Month'

The latest model of Apple's ultra-light MacBook Air is scheduled to hit the market by the end of this month, media in the computer manufacturing hub of Taiwan reported on Tuesday.

The first shipment of the next-generation MacBook Air - the thinnest line of Apple's notebook computers, shorn of a hard drive and disc player - will be 380,000 units, the Taipei-based Economic Daily News said.

An 11.6-inch model will account for 55 percent of the units in the first batch, and a 13.3-inch model the rest, according to the paper.

It said that about 90 percent of MacBook Airs would be assembled by Taiwan's Quanta Computer, a leading contract computer manufacturer.

Chrome, Firefox Browsers To Get Tighter PDF Integration

Browser developers at Google and Mozilla are working on new ways to more

tightly integrate PDF capabilities. Google was the first browser maker to integrate a PDF reader in Chrome instead of a plug-in vulnerable to hacker attacks. Now Chrome developers have taken the next step.

A new print-preview function in Chrome 13 beta lets web surfers convert any web page into a PDF file. Users on a Wi-Fi-only notebook, media tablet, or PDF-compatible e-reader should find this capability useful because web content can now be stored as PDF files for later reading where hot-spot access is unavailable.

"Print preview uses Chrome's built-in PDF viewer to display the page you want to print, and it updates automatically as you adjust your print settings," noted Google software engineer Chris Bentzel. "You can also choose to save any web page as a PDF file, using the 'Print to PDF' option that's automatically included in the printer list."

Using print preview is a straightforward process. Users encountering a web page they wish to print can click on the tool icon in the upper right corner of the Chrome 13 browser to select the print menu option. Print preview automatically appears in a separate window that shows users what the web page currently being viewed will look like when printed.

The Print To PDF option is among the available selections in the drop-down menu next to the word "destination." Users can even specify a single page or pages of content to be printed from among those displayed in the preview window. Click the Print button to save the selection as a PDF file.

Chrome's lack of a print-preview function has been among the top Chrome user requests since Google started requesting user feedback in 2008, according to Bentzel. Having finally implemented it on Windows and Linux, the Mac version will be coming soon. "Thanks for being patient with us on this one!" Bentzel added.

Mozilla's developer community is working to eliminate the use of a native-code PDF plug-in from Adobe Systems by building a secure PDF rendering engine into future Firefox browser releases. However, the developers are approaching the problem in an entirely different way than Google's developers.

"Google's Chrome browser goes through quite some pain to sandbox the PDF renderer to avoid code-injection attacks," Mozilla researcher Andreas Gal wrote in a blog. "An HTML5-based implementation is completely immune to this class of problems."

Firefox developers are working on a new open-source specification dubbed pdf.js for rendering PDF files quickly and securely from within the browser that is based on HTML5/JavaScript coding.

"Our most immediate goal is to implement the most commonly used PDF features so we can render a large majority of the PDF files found on the web," Gal wrote. "We believe we can reach that point in less than three months. The entire code so far is less than one month old, and it already renders a large set of PDF features."

Steve Jobs Comic Book Coming in August

Does Steve Jobs' black turtleneck have magical powers? Not exactly, but the Apple chief is getting his own comic book, which will hit stores in August.

Unfortunately, Jobs will not be getting a superhero name. The plainly titled "Steve Jobs: Co-Founder of Apple" will provide readers with "a unique insight into the Apple CEOs legendary drive to the top and his continuing fight to stay there," according to publisher Bluewater Productions.

"Admire him or hate him, Jobs' vision and business acumen revolutionized the world," said writer CW Cooke. "Between he and Microsoft founder Bill Gates, you would be hard pressed to find someone with greater influence over how we communicate, interact and do business over the last 30 years."

The 32-page comic book was drawn by Chris Schmidt, while the cover art was created by DC artist Joe Phillips. It will be available in comic shops and bookstores, as well as online via Amazon, Barnes & Noble, and Borders for $3.99.

"His innovations command front page news, speculation of his health affects the stock market. Not bad for a college dropout," Bluewater president Darren Davis said in a statement. "His story, and that of Apple, is epic. I'm surprised it took us this long to publish a proper, balanced biography of him."

Bluewater is also behind the 48-page Mark Zuckerberg comic book, which was written by Jerome Maida and illustrated by Sal Field. The company said the success of the Zuckerberg comic book inspired it to focus on Jobs. A graphic novel version of the Zuckerberg comic book will be in stores in September for $10.99.

"There are definitely some similarities between Zuckerberg and Jobs. It takes a certain kind of drive and a certain kind of genius to move society the way they have," said Cooke. "The idea behind both efforts is to show the person behind the personality and that it is never what you'd expect."

Bluewater has also tackled politicians and pundits. "Political Power: Glenn Beck" was released on April 6, and the company plans to release "Political Power: Republicans," which will focus on GOP headliners like Sarah Palin, Arnold Schwarzenegger, and Rush Limbaugh, in October. A version focused on Democrats, "Political Power: Democrats," will be available in September, focusing on politicians like Hillary Clinton, President Barack Obama, Senator Al Franken and the late Ted Kennedy.

JK Rowling Launches New Harry Potter Website

Harry Potter creator J.K. Rowling has launched a new website called "Pottermore," but fans of the boy wizard will have to wait to see what it entails as the entry page says simply "Coming Soon...."

The site, www.pottermore.com, was launched a month ahead of the release of the eighth and final Potter movie on July 15.

Some Potter fan sites, which have been instrumental in generating a

large and loyal fan base for the movies and seven-book series on which they are based, were given a sneak preview of the mysterious new website.

"It is, in a word, breathtaking," wrote Leaky Cauldron, one of the leading Potter sites. "That is all we are permitted to say at the moment."

Rowling and Potter studio Warner Bros. have never shied away from building up the hype ahead of key releases in the series.

The Harry Potter novels have sold more than 400 million copies worldwide, while the seven movies released so far have grossed some $6.4 billion in ticket sales. Rowling has been billed the "world's first billionaire author."

A spokeswoman for Rowling confirmed that the site was genuine.

"We can confirm that Pottermore is indeed the name of J.K. Rowling's new project. She will be announcing it soon," she said. "It is not a new book, but we won't say more than that!"

Put A Cork in The Internet Bubble Talk - For Now

It's starting to feel like a 1999 flashback. Internet companies - some of them profitable, some not - sense a golden opportunity and are lining up to go public this year.

But here's something to keep in mind as the latest case of Internet fever grips Wall Street: It's still nowhere close to the giddy days of the dot-com boom, when investors bought stocks as impulsively as lottery tickets. Technology stocks today are the cheapest in more than nine years, at least judging by one benchmark for appraising companies.

This year could yield the most initial public offerings of technology stocks since 2000. But the venture capitalists who bankroll high-tech startups aren't pouring money into the Internet like they once did. And even rapidly growing Internet companies LinkedIn Corp. and Pandora Media Inc. have lost some of their luster after dazzling investors when they went public in recent weeks.

All those factors signal that cooler heads are prevailing, especially with the global economy on shaky ground.

So far this year, 28 of the 74 IPOs completed in the U.S. have been by technology companies, according to IPO investment advisory firm Renaissance Capital. If, as expected, another 31 tech IPOs are completed by the end this year, it will be the most from the sector since 2000.

The growing enthusiasm for Internet services reflects how far the Internet has come since the dot-com boom. An estimated 2 billion people worldwide have Web access now, about eight times as many as in 2000. High-speed Internet connections have become common, turning the Web into an entertainment center as well as an information hub. And mobile devices have made it possible to stay connected from almost anywhere at any time.

"I don't see a bubble," venture capitalist Marc Andreessen, best known as founder of the pioneering Web browser Netscape, told The Associated

Press in March. Andreessen has investments scattered all over the Internet, mostly in companies that are steadily increasing their revenue. Some of them are even profitable, virtually unheard of during the late 1990s. That's why he thinks it's logical for more money to be flowing into one of the most promising parts of the U.S. economy.

"I think people are confusing success with a bubble," Andreessen said. "Maybe stuff is just working."

But well-established technology companies, including many that helped build the Internet into what it is today, have fallen out of favor. To gauge just how far, consider the price-to-earnings, or P/E, ratio of technology stocks in the bellwether Standard & Poor's 500 index.

The P/E number divides a company's stock price by its earnings per share. The higher the P/E, the more likely a stock is overvalued by the market. Based on earnings reported for the past year, the figure for S&P 500 tech stocks is 14.1, the lowest since March 2002. Before the Great Recession started in December 2007, it was 25.4. Before the Internet bubble blew up, it was 66.4.

Even Google, the Internet's most profitable company, hasn't been getting any love of late. Though its earnings are still rising at a robust rate, the company's stock has fallen more than $100, or 18 percent, so far this year.

LinkedIn, which runs a site for professional networking, triggered talk of another dot-com boom when its shares more than doubled in its stock market debut. LinkedIn was minted with a market value of $9 billion, the highest for an Internet company since Google went public in 2004.

Then Pandora Media, an Internet radio station, doubled the target price for its IPO because of such intense demand. At the end of its first day of trading Wednesday, Pandora had a market value of $2.8 billion - more than AOL Inc., which had a market value of more than $160 billion in early 2000.

Pandora stock fell below its IPO price of $16 in its second day on the market, suggesting investors were having second thoughts about a company that still hasn't turned a profit despite building an audience of 94 million. In another indication of sobriety, LinkedIn's stock has lost more than a quarter of its value since its first day of trading.

The caution may be short-lived, though. Online coupon seller Groupon Inc. has filed plans for an IPO that has analysts wondering whether its market value will exceed $25 billion - even higher than Google on the day it went public.

Groupon's revenue is growing at a much faster rate than Google's was when it went public. Unlike Google, though, Groupon has been losing money - $413 million last year.

When Groupon executives start meeting with prospective IPO investors, they could face questions about why the company's insiders decided to sell so many shares of what is supposed to be a great stock. Since April 2010, the insiders sold $860 million of stock, according to documents filed with the Securities and Exchange Commission. The sales generated windfalls of $382 million for Groupon co-founder Eric Lekofsky and $28 million for co-founder and CEO Andrew Mason. Both men remain among Groupon's largest shareholders. The company's IPO is expected in

September or October.

Other highly anticipated Internet IPOs on the horizon include Zynga, the maker of popular Web games such as "CityVille," and Facebook, which, with an audience of more than 500 million users, makes it the most likely candidate to turn the current Internet fever into delirium. Facebook, which was founded seven years ago in a Harvard University dorm room and could go public by next spring, has already been valued by private investors at $85 billion.

Adults Dominate as U.S. Social Networking Rises

Forty-seven percent of all social-networking users in the U.S. are adults over age 35, while just 16 percent are ages 16 to 22, according to the Pew Internet and American Life Project. The research center reported that social-networking activities have nearly doubled since 2008 by attracting older users.

What’s more, the amount of time users devote to social networking has grown dramatically. Users spend an average of 16.6 percent of their online time at social-networking sites, up from 8.3 percent in 2007, noted Andrew Lipsman, senior director of marketing and industry analysis at comScore.

Though the increase in time is no big surprise, what’s very interesting is the rapidly changing dynamics of the market, Lipsman observed. "For a long time, the social-networking story was almost exclusively the horse race between Facebook and MySpace," he wrote in a blog. "Tumblr is clearly experiencing a viral adoption curve right now."

Tumblr may be nearing the critical-mass threshold that has propelled other social-media sites to more widespread adoption, Lipsman noted. "It still has a ways to go before we can mention it in the same breath as LinkedIn or Twitter, but it just might get there if it maintains its current trajectory," he wrote.

Though Facebook continued to lead the field by attracting 157.2 million U.S. visitors in May, comScore noted that Tumblr (10.7 million visitors) and other leading social-networking players also reached all-time U.S. audience highs last month, including LinkedIn (33.4 million) and Twitter (27 million).

"There is definite underlying strength in LinkedIn’s user-adoption curve at the moment," Lipsman observed. "In fact, it has reached all-time U.S. audience highs in seven of the past 12 months and has grown 58 percent overall in the past year."

Moreover, the number of visitors at Twitter has increased 13 percent year over year, which Lipsman attributed in part to the "exceptionally buzz-worthy news story of Osama Bin Laden’s death" as well as an ongoing discussion of the royal wedding. However, the most impressive gains during the past year have been made by Tumblr, which racked up 166 percent growth.

Though MySpace continues to be the second most popular social-networking site for U.S. users after Facebook, its audience has declined nearly 50 percent during the past year. Moreover, the length of the average user

engagement at MySpace has dropped 85 percent, Lipsman observed.

According to Pew, 92 percent of all U.S. social-network users were on Facebook when the survey was conducted in October and November of 2010. Only 29 percent used MySpace, followed by LinkedIn (18 percent) and Twitter (13 percent).

However, only seven percent of MySpace users and six percent of LinkedIn users said they accessed these sites on a daily basis, Pew reported. By contrast, 52 percent of Facebook users and 33 percent of Twitter users reported daily access.

Compared with Internet users in general, Facebook users accessing the site multiple times per day were 250 percent more likely to attend a political rally or meeting. Moreover, 57 percent were more likely to have tried to convince someone to vote for a specific candidate, and 43 percent were more likely to say they would vote.

By contrast, those who use MySpace have a significantly higher ability to consider multiple points of view. "The average adult scored 64/100 on a scale of perspective taking," Pew researchers noted. "A MySpace user who uses the site a half-dozen times per month tends to score about eight points higher on the scale."

Juror Faces Jail for Facebook Chat with Defendant

A British juror will be sent to jail for discussing a drug and corruption trial with a defendant on Facebook, a judge said Tuesday.

Justice Igor Judge told Joanne Fraill - the first juror in Britain to be convicted for using the Internet during a trial - that she would get a prison term when she is sentenced later in the week. The maximum sentence for contempt is two years in jail

Prosecutors say Fraill and defendant Jamie Sewart communicated on the social networking site during the trial last year, with Sewart asking Fraill for details of the jury’s deliberations.

Sewart, 34, was acquitted at that trial but later charged with contempt.

Fraill pleaded guilty to contempt, acknowledging that she communicated with Sewart and also researched the case online while serving on the jury.

According to The Guardian newspaper, in one exchange Sewart asked Fraill how deliberations were going and Fraill replied: "Cant get anyone to go either no one budging pleeeeeese don’t say anything cause jamie they could all miss trial."

Defense lawyer Peter Wright said 40-year-old Fraill was "distraught at what she had done, wholly contrite and remorseful."

He said she contacted Sewart because she felt the two had a lot in common.

"Her conduct, though reprehensible, was not calculated or designed by her to subvert the trial process, although it is conceded that that was an inevitable consequence of it," Wright said.

Sewart had denied contempt but was found guilty Tuesday by judges at London’s High Court.

While Fraill is going to prison, Sewart was told she would receive a suspended prison sentence because she has a young child, from whom she was separated during her original trial

The panel of three judges also will hear an appeal by one of the convicted defendants, who wants his sentence overturned on the grounds of jury misconduct.

Jurors in British trials are warned not to talk to anyone about their case, or to research it on the Internet.

The attorney general’s office said the case was Britain’s first contempt prosecution involving use of the Internet by a juror.

".brands" Approach with Internet Name Shake-up

Brand owners will soon be able to operate their own parts of the Web - such as .apple, .coke or .marlboro - if the biggest shake-up yet in how Internet domains are awarded is approved.

After years of preparation and wrangling, ICANN, the body that coordinates Internet names, is expected to approve the move at a special board meeting in Singapore on Monday.

Today, just 22 generic top-level domains (gTLDs) exist - .com, .org and .info are a few examples - plus about 250 country-level domains like .uk or .cn. After the change, several hundred new gTLDs are expected to come into existence.

The move is seen as a big opportunity for brands to gain more control over their online presence and send visitors more directly to parts of their sites - and a danger for those who fail to take advantage.

It will also change the way search engines like Google find results, and the way organizations use search-engine optimization to improve the visibility of their websites in search results.

"As a big brand, you ignore it at your peril," says Theo Hnarakis, chief executive of Australian domain name-registration firm Melbourne IT DBS, which advises companies and other organizations worldwide about how to do business online.

"We’re advising people to buy their brands, park them and redirect visitors to their existing site, at the very least," says Hnarakis, whose more than 3,500 customers include Volvo, Lego and GlaxoSmithKline.

If the change is approved on Monday, applications are likely to open in January for a 90-day period before closing again, potentially for years.

It will cost $185,000 to apply, and individuals or organizations will have to show a legitimate claim to the name they are buying. ICANN is taking on hundreds of consultants to whom it will outsource the job of adjudicating claims.

"The commercial participants are the most active, aggressive and articulate members of our society," ICANN CEO Rod Beckstrom told Reuters in a recent interview, saying trademark owners in particular were anxious about how the new regime would work.

As well as big brands, organizations such as cities or other communities are expected to apply.

GTLDs such as .nyc, .london or .food could provide opportunities for many smaller businesses to grab names no longer available at the .com level - like bicycles.london or indian.food.

The new domains will also change how ICANN works, as it will have a role in policing how gTLDs are operated, bought and sold. Until now, it has overseen names and performed some other tasks but has been little involved in the Internet’s thornier issues.

To prevent so-called cyber-squatting, gTLD owners will be expected to maintain operational sites. ICANN will have to approve transfers to new owners at the top level.

=~=~=~=